Title (en)

Method and apparatus for implementing hierarchical electronic cash

Title (de)

Verfahren und Vorrichtung zum Einführen von hierarchischem elektronischem Geld

Title (fr)

Méthode et dispositif pour la mise en oeuvre de la monnaie électronique hiérarchique

Publication

EP 0810563 A3 20000105 (EN)

Application

EP 97108325 A 19970522

Priority

JP 13516796 A 19960529

Abstract (en)

[origin: EP0810563A2] A user U generates a signature verification key NU, a signature key SSU and a cipher key K, enciphers (X,NU) by a public key into EI(X,K,NU) and sends the enciphered information to a bank together with user information U and the amount of money X. The bank registers the information U and EI in a user data base in correspondence with each other, then withdraws the amount of money X from a user's bank account and sends information (X,EI) to an electronic cash issuer together with a bank signature SB(X,EI) for the information. The issuer deciphers the enciphered information EI by a secret key to obtain the information (X,NU), then registers the information EI and the key NU in an inspection data base in correspondence with each other, and enciphers the signature SI(X,NU) attached to the key NU by the key K into EK(SI), which is sent to the user via the bank. The user deciphers the information EK by the key K to obtain the issuer signature SI and sends to a shop, as electronic cash C, information containing the key NU and the issuer signature SI. The shop verifies the validity of the issuer signature and the suer signature and, if they are valid, approves payment in an amount y. The shop sends data H of communication with the user to the issuer for settlement of accounts, and the issuer makes a check to see if the key NU in the data H is registered in the inspection data base. <IMAGE>

IPC 1-7

G07F 19/00; G06F 17/60; H04L 9/32

IPC 8 full level

H04L 9/32 (2006.01); **G06Q 10/00** (2012.01); **G06Q 20/00** (2012.01); **G06Q 20/06** (2012.01); **G06Q 20/30** (2012.01); **G06Q 20/36** (2012.01); **G06Q 20/40** (2012.01); **G06Q 20/42** (2012.01); **G06Q 40/00** (2012.01); **G06Q 40/02** (2012.01); **G06Q 50/00** (2012.01); **G07F 7/10** (2006.01); **G09C 1/00** (2006.01)

CPC (source: EP US)

G06Q 20/02 (2013.01 - EP US); **G06Q 20/06** (2013.01 - EP US); **G06Q 20/085** (2013.01 - EP US); **G06Q 20/10** (2013.01 - EP US); **G06Q 20/102** (2013.01 - EP US); **G06Q 20/3678** (2013.01 - EP US); **G06Q 20/3829** (2013.01 - EP US); **G06Q 20/383** (2013.01 - EP US); **G06Q 20/40** (2013.01 - EP US); **G06Q 40/00** (2013.01 - EP US); **G06Q 40/12** (2013.12 - EP US); **G07F 7/1016** (2013.01 - EP US); **H04L 9/3247** (2013.01 - EP US); H04L 2209/56 (2013.01 - EP US)

Citation (search report)

- [A] US 5455407 A 19951003 - ROSEN SHOLOM S [US]
- [A] US 5511121 A 19960423 - YACOBI YACOV [US]
- [XPA] WO 9641316 A2 19961219 - KRAVITZ DAVID W [US], et al
- [A] BRANDS S: "ELECTRONIC CASH ON THE INTERNET", PROCEEDINGS OF THE SYMPOSIUM ON NETWORK AND DISTRIBUTED SYSTEM SECURITY,XX,XX, PAGE(S) 64-84, XP000567597
- [A] TATSUAKI OKAMOTO: "AN EFFICIENT DIVISIBLE ELECTRONIC CASH SCHEME", PROCEEDINGS OF THE ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE (CRYPTO),DE,BERLIN, SPRINGER, VOL. CONF. 15, PAGE(S) 438-451, ISBN: 3-540-60221-6, XP000565124
- [A] MEDVINSKY G ET AL: "NETCASH: A DESIGN FOR PRACTICAL ELECTRONIC CURRENCY ON THE INTERNET", ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY,XX,XX, pages 102-106, XP000604414
- [AP] "NEW ELECTRONIC MONEY SYSTEM", NTT REVIEW, vol. 8, no. 6, 1 November 1996 (1996-11-01), pages 4, XP000642071

Cited by

US6539364B2; EP0886248A3; EP1197927A3; EP0926637A3; US7418425B2

Designated contracting state (EPC)

DE FR GB

DOCDB simple family (publication)

EP 0810563 A2 19971203; **EP 0810563 A3 20000105**; JP 3329432 B2 20020930; JP H09319808 A 19971212; US 5926548 A 19990720

DOCDB simple family (application)

EP 97108325 A 19970522; JP 13516796 A 19960529; US 85921497 A 19970520